

**Taniyama's conjecture is wrong. Andrew Wiles could not solve the Fermat problem!**

**N.Z.Orujov**

*(Educational center Master NR 1, Baku, Azerbaijan)*

**Z.S.Orujov**

*(School No1 named after I. Ibrahimov,  
Yukhari Khalaj village of Salyan region,  
Azerbaijan)*

It is known from the history of mathematics that the complete solution of the Fermat problem is based on the Japanese mathematician Yutaka Taniyama's conjecture (1955). According to this conjecture, every elliptic curve can be shown by modular functions and the formula is as follows.

$$y^2 = x(x - a^n)(x - b^n) \quad *$$

Here  $a$  and  $b$  are rational numbers.

In 1985 the german mathematician Gerhard Frey assumed that for the curves \*, the Fermat theorem can be derived as a corollary from the well-posedness of this conjecture. In 1986 K.A. Ribet proved that there is no Frey elliptic curve in the case when the Taniyama conjecture is well-posed. So, to prove the Fermat theorem it remained to prove the Taniyama conjecture. This was realized by Andrew Wiles.

But the Taniyama conjecture is not true for every elliptic curve. Its proof is as follows.

**Example:** for  $t_0$  being any rational number, solve the equation  $u^2 - v^2 = t_0$  in the set of rational numbers.

**Solution:** It is clear that by the infinitely many method any rational number can shown as the product of two numbers. I.e.  $t_0 = \frac{t_0}{q} \cdot q$ ,  $q$  is a rational number.

Denote  $\frac{t_0}{q} = p$ . Then  $(u - v)(u + v) = pq \Leftrightarrow \begin{cases} u - v = p \\ u + v = q \end{cases} \Leftrightarrow u = \frac{p + q}{2}, v = \frac{p - q}{2}$ . So,

the equation  $u^2 - v^2 = t_0$  has always a solution in the set of rational numbers and their number is infinitely many. Writing the values of  $u$  and  $v$  in the equation, we

obtain the identity  $pq = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$ . Assume that  $a$  and  $b$  being any rational numbers, the numbers  $a^n$  and  $b^n$  are given. ( $n \in \mathbb{N}$ ). Let us consider the difference  $a^n - b^n$ . It is clear that this difference also will be a rational number and we denote it by  $t_0$ .  $a^n - b^n = t_0 = u^2 - v^2$  is valid. Hence we obtain  $a^n - u^2 = b^n - v^2$ . These differences are also rational numbers and we denote them by  $x$ .  $a^n - u^2 = b^n - v^2 = x$ . Then  $u^2 = a^n - x$  and  $v^2 = b^n - x$ . We have noted that since the number of the variables  $u$  and  $v$  is infinitely many the number of  $x$  is also infinitely many. If we multiply these equalities side by side, we obtain  $(uv)^2 = (a^n - x)(b^n - x) = (x - a^n)(x - b^n)$ . Denoting  $uv = y$  and considering it as an independent variable, we get the equation

$$y^2 = (x - a^n)(x - b^n) \quad \oplus$$

For any fixed rational numbers  $a^n$  and  $b^n$ , this equation always has a solution and their number is infinitely many. So, we proved that any elliptic curve can be shown by modular functions in the form of  $\oplus$ . Comparing the equations  $\oplus$  and  $*$ , we determine that in the equation  $*$  the variable  $x$  is an excess (additional) factor. I.e. the equation in the conjecture is a cubic equation, but we proved that it is a quadratic equation. Thus the Frey conjecture, Ribet's proof fails. As can be seen, we did not analyze the Wiles "proof", we  $\oplus$  directly proved that the conjecture is expressed by the equation  $\oplus$  of the conjecture.

And also, the elliptic equation that expresses the conjecture, can be in the form of

$$y^2 = (x - a^n)(x + b^n) \quad \oplus'$$

as well. Let us show this. Again, similarly

$$a^n + b^n = u^2 - v^2 \Leftrightarrow a^n - u^2 = -b^n - v^2 = x \Leftrightarrow a^n - x = u^2, -b^n - x = v^2.$$

Multiplying these equalities side by side and accepting  $uv = y$ , we obtain the equation  $\oplus'$ . When  $n$  is an odd natural number, in the equation  $\oplus'$  replacing  $b$  by  $-b$ , the equations  $\oplus$  and  $\oplus'$  become the same equations.

By when  $n$  is an even number, the equations  $\oplus$  and  $\oplus'$  do not coincide, i.e. they are different. In a word, the conjecture is expressed by the equations  $\oplus$  and

$\oplus'$ . Thus, Taniyama's conjecture is wrong. Andrew Wiles could not solve the Fermat theorem.

**Serious signal.** The scientists that engage in algebra, geometry and number theory should not refer in their works to Taniyama's conjecture. Otherwise, they will obtain wrong results. Only the equations  $\oplus$  and  $\oplus'$  can be used. The Beal and Fermat problems were fundamentally solved in the following paper.

## THE BEAL CONJECTURE AND ITS SOLUTION

When in the Fermat equation  $x^n + y^n = z^n$  the exponent is different, i.e.  $x^k + y^n = z^m$ , does the equation has a solution in the set of natural numbers?

As is seen, the equation has six unknowns. The equation belongs to the class of Diophantus equations.  $76^2 - 7^4 = 15^3$ ,  $7^3 - 10^2 = 3^5$  and so on. We can show a great number of such equations. In the equalities the basis are pairwise co-prime numbers. But one of the powers is less than 3, i.e. is 2. In another example  $70^3 + 105^3 = 35^4$  the powers are greater than two, but the bases of the power are not one-to-one prime numbers  $(70; 105; 35) = 35$ . The common multiplier is 35.

The equation  $x^k + y^n = z^m$  being a special case of the equation  $x^n + y^n = z^{n+1}$  has the following solutions.  $x = a(a^n + b^n)$ ,  $y = b(a^n + b^n)$ ,  $z = a^n + b^n$  ( $a; b; n \in N$ ).

But the common multiplier is  $a^n + b^n$ . For natural numbers  $n > 2$  an infinite number of solutions are obtained.

So, Andu Beal is fair to express the problem in the following form, i.e. when  $m, n, k$  (powers) are greater than two and  $x; y; z$  (bases of powers) are pair-wise co-primes has the equation  $z^m - x^k = y^n$  (Beal equation) solutions? This means that we must show even one example that satisfies the Beal condition, or prove that the Beal equation has no solution. We choose the second way.

Assume that the equation  $u - v = h$  with three unknowns was given ( $h$  is an odd natural number).

**I.** Find all natural numbers solutions of the equation  $u - v = h$ .

**II.** Are there  $u_0, v_0$  and  $h_0$  natural numbers among the solution of this equation then we get  $u_0 = z_0^m, v_0 = x_0^k$  and  $h_0 = y_0^n$  ( $z_0, x_0, y_0 \in N, m, n, k$  are the natural numbers greater than 2) that is  $x_0^k + y_0^n = z_0^m$  equation is obtained.

so we stated the Beal Problem.

According to the Beal terms, X and Y cannot be even natural numbers at the same time. At least one of them is an odd natural number. Hereinafter, we will take Y as an odd natural one.

**Example 1.** when  $h = b_0$  is not an arbitrary odd natural number, find natural solutions of the equation  $u - v = b_0$ :

**Solution:** It is obvious that  $u - v$  is a constant. The sum  $u + v$  always changes. We denote it by a  $u + v = a$  ( $a > b_0$ ). Then necessarily the system of linear equations  $\begin{cases} u - v = b_0 \\ u + v = a \end{cases}$  is formed. We get  $u = \frac{a + b_0}{2}, v = \frac{a - b_0}{2}$ . Since  $b_0$  is an arbitrary odd number, we denote it by b.

Then we get the system of equations  $\begin{cases} u - v = b \\ u + v = a \end{cases} \quad \begin{matrix} b \neq 1 \\ a > b \end{matrix} \quad (A).$  Again the solutions

$u = \frac{a + b}{2}, v = \frac{a - b}{2}$  are obtained. It is obvious that these solutions are not only the solution of the equation  $u - v = b$  but also of the equation  $u + v = a$ . These equations are pairs. In the solution of the equation  $u - v = 1$  there remains one  $u + v = ab$  case. We add it and get the system of equations.  $\begin{cases} u - v = 1 \\ u + v = ab \end{cases} \quad (B).$   $u = \frac{ab + 1}{2}; v = \frac{ab - 1}{2}$ . As can be seen, the set of solutions of  $u - v = h$  linear Diophantine equation is the connection of the set of solutions of A and B system of linear equations.

Multiplying the equations in the A and B system, we get the quadratic equation  $u^2 - v^2 = ab$ . The set of its solutions is in the form

$$\left\{ \left( \frac{a+b}{2}; \frac{a-b}{2} \right) \right\} \cup \left\{ \left( \frac{ab+1}{2}; \frac{ab-1}{2} \right) \right\}. \text{(new solutions neither are formed nor}$$

lost). Denoting  $ab = t$ , we structure a new equation with three unknowns  $u^2 - v^2 = t$ . It means that the equation  $u - v = h$  and the equation are equivalent equations in the set of natural numbers. We say that without changing the set of solutions of the equation  $u - v = h$ , we changed its form. Therefore we will look for the solutions of the Beal equation among the solutions of the equation  $u^2 - v^2 = t (t > 1)$ . So  $z^m = u^2, x^k = v^2$  and  $t = y^n$

**Example 2.** For an odd natural number  $t > 1 \forall$  find the natural solutions of the equation  $u^2 - v^2 = t$  satisfying the condition  $(u; v) = 1$ .

**Solution.** If  $t$  is an odd number, one of the natural numbers  $u$  and  $v$  is odd the another one is even. Then  $u + v$  and  $u - v$  are odd numbers. As  $(u; v) = 1, (u + v; u - v) = 1$ . Indeed, if  $(u + v; u - v) = d$  ( $d > 1$  is an odd number), then there must be  $u + v = dk_1$ ,  $u - v = dk_2$  ( $k_1; k_2$ ) = 1.

Hence we get  $2u = d(k_1 + k_2)$  and  $2v = d(k_1 - k_2)$  i.e.  $u$  and  $v$  is divided by  $d$ .

This contradicts the condition  $(u; v) = 1$ . Thus, if  $(u; v) = 1$ , then  $(u + v; u - v) = 1$ . As

$t = u^2 - v^2 = (u + v)(u - v)$  there exist co-prime odd numbers  $a$  and  $b$  such

$$\text{that } \begin{cases} t = ab \\ u + v = a \\ u - v = b \end{cases} \cup \begin{cases} t = ab \\ u + v = ab \\ u - v = 1 \end{cases} \quad \begin{matrix} \Downarrow \\ \Downarrow \end{matrix}$$

$$\begin{cases} t = ab \\ u = \frac{a+b}{2} \\ v = \frac{a-b}{2} \end{cases} \cup \begin{cases} t = ab \\ u = \frac{ab+1}{2} \\ v = \frac{ab-1}{2} \end{cases} *$$

We have determined that  $ab; \frac{a+b}{2}; \frac{a-b}{2}$  and  $ab; \frac{ab+1}{2}; \frac{ab-1}{2}$

numbers are pairwise co-primes for  $(a; b) = 1$  odd numbers. So, we obtain that when  $t$  is an odd number, the equation  $u^2 - v^2 = t$  always has a solution and it is expressed by formulas \*. If we substitute the values of  $u, v$  and  $t$  in the equation, we get the identity

$$ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2, ab = \left(\frac{ab+1}{2}\right)^2 - \left(\frac{ab-1}{2}\right)^2$$

These two formulas may be expressed in one formula.

$$cp = \left(\frac{c+p}{2}\right)^2 - \left(\frac{c-p}{2}\right)^2$$

If  $c = a$  and  $p = b$ , the first equation is obtained; and if  $c = ab$  and  $p = 1$ , the second one is obtained. We will express the identity with  $a$  and  $b$ , because it has no effect on the general condition:

$$ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

**Corollary .** For  $t = y^n$  ( $n > 1, n \in \mathbb{N}$ ), we get the equation  $u^2 - v^2 = y^n$ . Then all-natural solutions satisfying the condition  $(u; v) = 1$  of this equation are expressed by the formula

$$\begin{cases} y = ab \\ u = \frac{a^n + b^n}{2} \quad a > b \quad \forall (a; b) = 1. \\ v = \frac{a^n - b^n}{2} \end{cases}$$

We must recall that the numbers  $ab, \frac{a^n + b^n}{2}, \frac{a^n - b^n}{2}$  are pairwise co-primes. If we once clarify our mind, we can state that if the **Beal** equation has solutions, then they are among the solutions of the equation  $u^2 - v^2 = y^n$ .

**Lemma.** For any odd and even numbers  $z^m$  and  $x^k$  ( $z, x \in N, m, k$  are large natural numbers greater than 2) there exist such natural numbers  $(u; v) = 1$  and  $l \in N_0$  shown in the form  $z^m = u^2 \pm l$  and  $x^k = v^2 \pm l$ .

**Proof.** Let us take any even and odd numbers  $z^m$  and  $x^k$  ( $z^m > x^k$ ). Denote  $z^m - x^k = t$  ( $t$  is an odd number). According to example 2 we can state that there exist such natural numbers  $z^m - x^k = t = u^2 - v^2$  that  $(u; v) = 1$  i.e.  $|z^m - u^2| = |x^k - v^2| = l$  or  $z^m = u^2 \pm l, x^k = v^2 \pm l$ . The proof is complete.

**Theorem.** If under the given conditions the Beal equation  $z^m - x^k = y^n$  has solutions in the set of natural numbers, then there exist such odd numbers  $\exists(a; b) = 1$  and natural numbers  $l \in N_0$  that these solutions in the parametric form are expressed by the following formulas

$$\begin{aligned} y &= ab \\ z^m &= \left( \frac{a^n + b^n}{2} \right)^2 \pm l \quad (u > b) \\ x^k &= \left( \frac{a^n - b^n}{2} \right)^2 \pm l \end{aligned}$$

**Proof:** Apply the lemma to the Beal equation. Substitute the formulas  $z^m = u^2 \pm l, x^k = v^2 \pm l$  in the Beal equation. Then we get the set the known equation  $u^2 - v^2 = y^n$

$$u = \frac{a^n + b^n}{2}, v = \frac{a^n - b^n}{2}, y = ab$$

Having substituted the values of  $u$  and  $v$  in the formulas  $z^m = u^2 \pm l$  and  $x^k = v^2 \pm l$  we get the above formulas. If in these formulas we write  $l=0$  for any odd numbers  $y \in N(y=ab)$  of the Beal equation we get particular solutions

$$z^m - x^k = y^n \quad z_0^m = \left( \frac{a_0^n + b_0^n}{2} \right)^2, \quad x_0^k = \left( \frac{a_0^n - b_0^n}{2} \right)^2 \text{ and } y_0 = a_0 b_0$$

If these solutions exist, it has other solutions as well, and they are expressed by the formulas  $z^m = z_0^m \pm l$ ,  $x^k = x_0^k \pm l$ . If there are no such particular solutions, the other solutions are absent as well.

**Main result:** we will look for the solutions of the Beal equation in the form

$$y \in N(y=ab) \quad y=ab, \quad z^m = \left( \frac{a^n + b^n}{2} \right)^2 \text{ and } x^k = \left( \frac{a^n - b^n}{2} \right)^2 \text{ i.e. in the class } l=0.$$

Remind that for the odd numbers  $(a;b)=1$  the numbers  $ab; \frac{a^n + b^n}{2}; \frac{a^n - b^n}{2}$  are pairwise co-prime natural numbers i.e.  $y; z; x$  are pair-wise co-prime natural numbers. This satisfies the Beal condition. We again remind that the equation  $t^n = h^2$  ( $n > 2$ ) has infinite number of natural solutions. No matter whether the  $n$  is odd or even, if  $t_0^n = h_0^2$  is satisfied, then there exists number  $t_1 \in N$  that  $t_0 = t_1^2$  is valid.

**The Beal theorem:** For large natural numbers  $m; n$  and  $k$  greater that 2 the equation  $z^m - x^k = y^n$  has no pair-wise one-to-one simple solution.

**Proof.** Let us assume the contrary. Assume that there exists a triple of such pair-wise co-prime numbers  $(y_0, z_0, x_0)$  that the equality  $y_0^n = z_0^m - x_0^k$  is true. Then according to **Theorem(Main result)** we can state that there exists such odd natural numbers  $(a_0, b_0)=1$  that

$$\begin{cases} y_0 = a_0 b_0 \\ z_0^m = \left( \frac{a_0^n + b_0^n}{2} \right)^2 \\ x_0^k = \left( \frac{a_0^n - b_0^n}{2} \right)^2 \end{cases} \quad (a_0 > b_0)$$

Each of the equalities of the system is true. This means that  $\exists z_1; x_1 \in N$  such that  $z_0 = z_1^2$ ,  $x_0 = x_1^2$ .

$$\text{If we subtract } \begin{cases} z_1^m = \frac{a_0^n + b_0^n}{2} \\ x_1^k = \frac{a_0^n - b_0^n}{2} \end{cases}, \text{ we get } z_1^m - x_1^k = b_0^n.$$

Accept  $b_0 = y_1$ . We can write  $z_1^m - x_1^k = y_1^n$ . Here  $z_0 = z_1^2 \geq z_1$ . There can not be  $z_1^2 = z_1$ . If  $z_1^2 = z_1$  it has the roots  $z_1 = 0$  and  $z_1 = 1$ .

When  $z_1 = 0 \notin N$ ,  $z_1 = 1$ , we get  $z_1 = z_1^2 = 1$ . Then the equality  $y_0^n = 1 - x_0^k$  is not true in the set of natural numbers. So,  $z_0 > z_1$ . Thus, if we assume that the Beal equation has the solution  $(y_0, z_0, x_0)$ , we find the existence of the second solution  $(y_1, z_1, x_1)$ . If we continue this process by applying these formulas in **Theorem(Main result)**, we get the sequence of infinite solutions of the Beal equation  $(y_0, z_0, x_0); (y_1, z_1, x_1), (y_2, z_2, x_2) \dots$

It became clear that  $z_0 > z_1 > z_2 \dots$  is a sequence of monotonically decreasing numbers. It is known that the sequence of decreasing natural numbers less than  $z_0$  cannot be infinite. So, we get contradiction. This shows that the statement of the Beal theorem is true.

Thus, the Beal problem was proved in the general case.

**Special remark.** If in the Beal equation we write  $m = k = n > 2$ , we get the Fermat theorem.

**The final result:** The identity  $\left( \frac{a^n - b^n}{2} \right)^2 + (ab)^n = \left( \frac{a^n + b^n}{2} \right)^2$  solves the Fermat and

Beal problems